



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450,
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/454,646	12/06/1999	David Carroll Challener	RP9-98-055	4026

25299 7590 12/09/2003

IBM CORPORATION
PO BOX 12195
DEPT 9CCA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/09/2003

10

Please find below and/or attached an Office communication concerning this application or proceeding.

2

Office Action Summary

Application No.

09/454,646

Applicant(s)

CHALLENGER ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☒ The proposed drawing correction filed on 17 October 2003 is: a) ☒ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s) ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

Response to Amendment

1. Examiner withdraws the objections to the drawings as the proposed amendments to the drawings overcome the objections.
2. Examiner withdraws the objections to the title of the invention as the amended title overcomes the objection.
3. Examiner withdraws the objections to the specification as the amendments to the disclosure overcome the objections.
4. Examiner withdraws the objection to claim 3 as the amendment to the claim overcome the rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1-9 are rejected under 35 U.S.C. 102(a) as being anticipated by Frisch Essential System Administration 2nd Edition (hereinafter Frisch). Methodologies for establishing levels of security as disclosed by the applicant in the claims are found in several OS systems. The security system integrated in the Unix OS is an example. Referring to claims 1-6, Frisch teaches how Unix stores user profile information utilizing various methodologies. Users are given their own unique id and at least one group id,

Art Unit: 2132

wherein the ids define for each user a security access level (see Frisch, page 146). Moreover, user and group ids are located in the passwd and group files in the /etc/ directory of a Unix system (see Frisch, page 146). Associated with each user id are distinct usernames and passwords; this information is used in multiple security-driven events including user login and administration of file read, write, and execute permissions (see Frisch, pages 25-36). Of the users, the root user is afforded the highest security level and can read, write, and execute any file on the system, thereby enabling the root user to change both the passwd and group files (see Frisch, page 5). Moreover, only the root user can change the run level of the OS, which includes the following: run level 1 for system administration state, run level s for single-user mode, and run level 2 for multi-user mode (see page 90, Table 4-1). As such, only the root user can change the security of the system to a lower state. In addition, Unix enables a "normal user" (one without root access) to establish a more secure state. Examples of normal user defined activity include writing cron jobs to periodically log the account activity and changing file permissions on files owned by the user to more secure levels (see Frisch, pages 381-386 and pages 25-36). Furthermore, Frisch discloses a feature to log unsuccessful login attempts. Under the AIX version of Unix, the /etc/security/user file lists several login profile attributes for each user including: the time of the last login, unsuccessful login count, time of the last unsuccessful login, and the host machine of the last unsuccessful login (see Frisch, page 262, 'Monitoring unsuccessful login attempts'). Upon inspection of the /etc/security/user file, an administrator can deny a user having a suspicious login profile from accessing the operating system. The UNIX

OS also provides a feature to automatically allow or deny use of the personal computer based on the security profile (see Frisch, pages 158-159, '/etc/default/login', Table 5-1, variable='MAXTRYS'). Finally, applications of any electrical computing system are generated when the system is turned on; hence, the security profile is generated when the system is turned on.

7. Referring to claims 5 and 6, Frisch teaches a system for establishing a level of security in a computer having a memory and a stored operating system as outlined above in the claim 4 rejection above under 35 U.S.C. 102(a). Although Frisch does not teach using binary indicators to set the secure state level, binary fields are the standard in the industry for storing any digital information. As mentioned above, normal users can change file permissions they own to more secure states and the root user can alter the state of a system to less secure states by making file and login access less restrictive and by changing the run level of the OS. Both of these changes would be reflected in memory as binary manipulations. Hence, the aforementioned cover claims 5 and 6.

8. Referring to claims 7-9, Frisch covers a method of providing improved security in a personal computer having an operating system and a security profile as outlined above. As mentioned above, each user can modify the read, write, and execute permissions on files they own, wherein the root user is able to modify all files. Moreover, only the root user can change the run level of the OS. Finally, the

administrator can implement any one or combination of the following in response to a security risk: alter the permissions for a subset of the files to a more secure level, update the /etc/passwd and /etc/group files by deleting suspicious accounts, update the /etc/default/login file to enforce more stringent login and account access requirements and broaden the login monitoring system utilizing various logging features.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Frisch as applied to claims 7-9 above, and further in view of Schmidt U.S. Patent No. 5,912,621 (hereinafter Schmidt). Frisch covers a security methodology implemented in a personal computer as defined above in the claim 7-9 rejections under 35 U.S.C. 102(a). Frisch does not teach that a response by the operating system is made when the cover of the computer is removed. Schmidt teaches a computer system that is responsive to the removal of its physical encasing. Specifically, the invention disclosed by Schmidt is a computer cabinet security state detection system whereby an auxiliary state element changes state in response to the cover being opened. A state program is run when the auxiliary state element detects the cover being removed to poll the status

of the element. This state report is further submitted to security personal for examination (see Schmidt, col. 1, line 51-col. 2, line 7). Administrators would then be able to adjust the security profile if the report shows suspicious activity. It would be obvious to one with ordinary skill in the art at the time the invention was made to incorporate the computer cabinet security state detection system into a computer system with a UNIX operating system. Schmidt teaches motivation for such an implementation: physical threats should be addressed to prevent tampering of the physical devices of a computer in addition to conventional login and network intrusion detection systems, and thereby enable a more robust computer security system (see Schmidt, col. 1, lines 1-10 and lines 35-50).

Response to Arguments

11. Applicant's arguments filed on October 17, 2003 have been fully considered but they are not persuasive.

12. Applicant argues that the claimed invention "describes the generation of a 'security profile' in response to 'the system [being] turned on' ... " whereas the invention taught by Frisch does not. Under the broadest interpretation of the claim, in any electrical computing device, programs are technically generated when "the system is turned on". This interpretation has been made after considering the applicant's definition of the term "generate" in the specification. There are two places in the specification where the applicant mentions or implies any means of creating and/or generating a security profile. They are found on page 13, first paragraph, 4th sentence,

and page 14, second paragraph, 1st sentence. There is no mention of a generation of a security profile in response to the system being turned on that suggests an alternative interpretation from the broadest interpretation of the claim.

13. Applicant also argues that the invention covered by Frisch only discloses a security system for limiting access to portions of a computer. As stated above, Frisch also teaches a feature that automatically allows or denies use of a personal computer based on a security profile (see Frisch, pages 159-169, 'Table 5-1', variable 'MAXTRYS'). Furthermore, the security profile reflects features including the number of unsuccessful "power-on" password attempts and the time of day (see Frisch, Chapter 5, pages 159-169 and page 157, last sentence; page 262, 'Monitoring unsuccessful login attempts'). Finally, the examiner's interpretation of the term "power-on password" is based on the term used in the applicant specification, which reads as follows:

It is well known to have a "power-on" password on a computer system. Such a system allows an authorized user to identify himself as an authorized user by his entry of the power-on password, then access the data and the programs stored on the computer.
(Specification, page 2, 3rd paragraph)

14. Consequently, the invention disclosed by Frisch anticipates the applicant's invention as claimed.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



Jung W Kim



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/454,646
Art Unit: 2132

Page 9

Examiner
Art Unit 2132

Jk
December 4, 2003